Gartner

Research

Publication Date: 9 July 2008 ID Number: G00159301

MarketScope for Wireless LAN Intrusion Prevention Systems

John Pescatore, John Girard

The WLAN intrusion prevention system market grew threefold, to $119 million, in 2007 as more organizations look to tighten their wireless security. In a market that is at the early stages of maturity, innovation still is required.

WHAT YOU NEED TO KNOW

Wireless networks remain a potentially significant vulnerability for enterprises, as a continuing stream of wireless LAN (WLAN)-based security incidents demonstrates. Because most enterprises support WLANs, enterprises must ensure that vulnerability management and intrusion prevention processes are extended to cover wireless and wired networks. WLAN security monitoring is required to ensure that supported WLANs are kept secure and that users do not install their technologies where WLANs (or faster technologies, such as 802.11n) are not supported.

The major decision enterprises face is whether to use security-monitoring functions that are provided by the WLAN infrastructure vendor as integrated capabilities or whether to implement an overlay system that is deployed and managed separately from the operational WLAN system. At the extremes, the choices are straightforward: Enterprises that are not deploying WLANs and want to prevent their use, as well as enterprises that are locked into older WLAN technologies that don't support current Wi-Fi Protected Access 2 security levels, should consider overlay products. Enterprises that do not have the budget for overlay security systems, or that have little WLAN exposure or low security demands, can meet their needs with an integrated approach. Other organizations should employ the use cases cited in the vendor evaluations of this MarketScope to assist in making the optimal choice.

MARKETSCOPE

Most enterprises have moved rapidly from trying to keep WLANs out of their organizations to fully embracing them widely across all corporate facilities. For many security organizations, this shift has meant that the focus on WLAN security has moved from finding and disabling rogue access points (APs) to detecting and remediating misconfigured APs. In this environment, wireless security-monitoring products are used mostly as vulnerability assessment and management products, and only secondarily as intrusion prevention products. However, new wireless technologies, such as 802.11n, have broadened the types of WLAN modulations that need to be detected, and emerging forms of wireless communications (such as WiMAX and third generation) will continue this trend. Also, as the use of WLANs becomes increasingly mainstream, vulnerability-seeking attacks will increase, and intrusion prevention capabilities will be used more. So, although the wireless intrusion prevention system (WIPS) market has reached the early mainstream phase, it continues to be a dynamic market where new features are needed with each product release.

This MarketScope analyzes, through the first half of 2008, the performance of vendors that have focused on this market. Gartner's evaluation is based on (in order of importance) continuing discussions with Gartner clients that are using and evaluating these products, survey responses from the vendors and interviews with reference customers that were provided by the vendors. The ratings shown quantify Gartner analysts' opinions of each vendor's performance in the market and should be used as just one input in your buying decisions.

Market/Market Segment Description

The WLAN intrusion prevention system (IPS) market consists of products that organizations buy to meet their security needs for vulnerability assessments and the monitoring of WLANs, as well as in providing detection and active blocking of potential attacks. As enterprise use of WLANs has matured, the major requirements have shifted from detecting rogue APs to quickly detecting misconfigured legitimate APs. The radio frequency (RF) monitoring of WLANs also has proved necessary for managing the performance and capacity of WLANs, as well as in dealing with help desk calls when users report operational problems. This trend has increased the importance of WLAN system management capabilities (such as richer audit trails and the identification and location of interference sources) for buyers. However, as new wireless technologies, such as 802.11n and WiMAX, appear, the "rogue" problem will reappear, which means that intrusion prevention capabilities will remain important.

Gartner estimates that global revenue in this market grew from $40 million in 2006 to $119 million in 2007 and that it will reach $168 million by year-end 2008. We believe that the initial sales of WLAN IPS products have penetrated the Global 5000 market to a significant degree, and all tracked vendors have wins in large companies. Most sales have significant upsell opportunities; buyers typically make a minimum purchase for the locations that are considered most vulnerable, although WLANs and other wireless technologies continue to expand in scope. However, many enterprises (especially smaller businesses and highly distributed larger companies) will find that the wireless security monitoring capabilities that are built into WLAN vendor infrastructure offerings are sufficient for their needs. This will keep downward pressure on penetration and pricing. Overall, Gartner believes that WLAN IPS revenue will double again during the next two years.

Vendors in this market comprise WLAN infrastructure vendors that sell distinct WIPS solutions, as well as smaller vendors that sell only WLAN-monitoring capabilities. All vendors offer security monitoring, as well as WLAN performance and troubleshooting monitoring; however, in this MarketScope, the vendors are ranked first and foremost on their abilities to fulfill the core requirements of WLAN IPS. Vendors with other lines of business receive credit for financial strength, as applicable, but their strengths and challenges in the core requirements of the market ultimately define their ratings.

For a detailed description of the core capabilities of WLAN IPS produces, see "What to Look for in a Wireless Intrusion Prevention System."

Explanation of MarketScope Scores

The rankings of vendors derive from the weighted evaluation criteria listed in the evaluation section of this research. The final rating for each vendor corresponds to a score that defines Gartner's overall assessment.

Strong Positive

The vendor shows a strong balance of forward-thinking technological development and competitive dominance in the market. High name recognition combines with business-relevant solutions to sell the technology more effectively than other market players. Strong-positive vendors are defining and refining the market by their actions and are forcing other vendors to conform. In this market, a strong-positive vendor is seen as reducing the cost of implementing wireless security for current technologies, providing a path to easily deal with new threats and new wireless technologies, and being the leader in integrating with leading WLAN technology providers.

Positive

Positive vendors are better than average at attracting business and generating revenue, but their market share is markedly behind what we would expect from a real or theoretical strong-positive vendor. The position of positive vendors, in terms of seats and revenue, shows growth for at least two years in a row, but positive vendors do not lead the market. Their products are an excellent fit for the market in terms of features and functions but may not be the broadest or most complete. Positive WLAN IPS vendors meet all market needs but may not have the channel reach or R&D strength to be clearly ahead of the competition.

Promising

Promising vendors have good and appropriate technologies for the market, although their offerings are not as complete as those that would garner a positive rating. Promising vendors have reached a size (or their division in a larger company has reached a size) that offers some stability in a startup market. We expect to see sales moving and growth within the year of an evaluation but do not require a year-over-year growth record. The promising vendor is a stable choice in the market. This vendor can be a niche player but runs the risk of going stale if it does not have a road map to demonstrate an understanding of the market and of competitors. Promising WLAN security vendors have sufficient financial strength and R&D capability to rapidly grow, but they may not have executed on this strength.

Caution

Vendors in the caution category are stable in the market, although their products/services are not strong contenders, because they do not adequately address the core requirements for the market. Features are missing or incomplete. Road maps may show progress to build out the product/service during the next year, but, in our assessment, this will not alter the market position relative to other vendors in the MarketScope. WLAN security vendors that are rated as caution are not necessarily unstable, but they are not on course to pursue the market over the long run.

Strong Negative

The strong-negative vendor is in a rapidly deteriorating situation that involves one or more of these criteria: the loss of key people, key investors, income/finance and technology, and failures of the product/service reported to Gartner or the media. The vendor is unable to demonstrate a forward path that will remedy these problems so that purchasers will not be put at risk. Officially, this is a do-not-buy warning.

Inclusion and Exclusion Criteria

This MarketScope evaluates vendors that offer overlay WLAN IPSs, as well as WLAN infrastructure (APs and WLAN controllers) vendors that have integrated WLAN IPSs into their WLAN infrastructure components. To be included in this research, vendors must have a WIPS product that provides the functions listed below, must meet minimum revenue criteria for shipping products and must provide at least three reference customers that are making good production use of their products.

The technical capabilities of these vendors' products must include rogue detection (rogue APs, clients and ad hoc networks), monitoring of airwaves for attacks and misuse, the ability to detect misconfigured APs and wireless endpoints, and quality-of-service enforcement or spectrum optimization capabilities. Location determination, the ability to mitigate the security deficiencies of Wired Equivalent Privacy-based WLANs and the availability of client software to provide policy enforcement on laptops that are in external environments are highly weighted capabilities but were not used as inclusion criteria.

Two vendors were dropped from the previous MarketScope:

- Network Chemistry: This vendor was acquired by Aruba Networks and is tracked as Aruba. Aruba offers an infrastructure-based approach and an overlay WIPS capability.
- Newbury Networks: This vendor focuses on Wi-Fi location systems and location-based applications, such as asset tracking. Its security application (RF Firewall) does not compete in the WIPS market but can be used as a complement to WIPS.

Several vendors were not included in this MarketScope because they did not meet the inclusion criteria:

- AirPatrol: This is the first company in this market space to create a business model based primarily on licensing OEM software to third parties and has done so since 2006. Software revenue is generated from royalties that are based on OEM sales. The company manufactures a line of hardware sensors that complements its software, which provides another revenue stream. This vendor's products did not enter the market under its own brand until April and May 2008, which means they have been available generally for only a few months, while other vendors in this research have had products in the field for several years. Customer feedback to Gartner regarding AirPatrol was positive, but this was based on preproduction systems. We will reassess AirPatrol in 2009, when its market presence has had time to mature.
- Meru Networks: This vendor sells production access systems mainly in competition with Cisco and Aruba. It developed patented "collision" methods for blocking unauthorized access to WLANs that are not breakable by hacking techniques. Meru does not, however, use its security features as a selling point, which becomes obvious when visiting its Web site. Meru does not have a stock-keeping unit for IPS and does not track the use of IPS; therefore, the company was unable to provide the financial and market share information needed to qualify for inclusion. To be competitively ranked in this MarketScope, Meru must position itself as an IPS competitor and must provide comparative revenue and sales data.

Rating for Overall Market/Market Segment

Overall Market Rating: Positive

We rate this market as "positive," because there will be a strong demand for WIPS products to further improve the security of wireless networks. Several established vendors are offering products on their own or in partnership with startup vendors. In addition, established and new vendors are continuing to innovate, especially in the area of intrusion prevention. We expect several partnerships to emerge among WLAN IPS and WLAN infrastructure vendors, and among wired and WIPS vendors.

Gartner estimates that the WLAN IPS market was worth about $40 million in 2005; this was expected to double in 2006.

Evaluation Criteria

Table 1. Evaluation Criteria

Evaluation Criteria	Comment	Weighting
Customer Experience	This includes the simplicity and flexibility of the product range, as well as ease of deployment, operation and support capabilities. This criterion was assessed by conducting qualitative interviews with vendor references and by obtaining feedback from Gartner clients.	high

Evaluation Criteria	Comment	Weighting
Offering (Product) Strategy	The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set as they map to current and future requirements.	high
Overall Viability (Business Unit, Financial, Strategy, Organization)	Viability includes an assessment of the overall financial health of the organization and its commitment to the WIPS market, along with the financial and practical success of the business unit. Also included is the likelihood of the organization/business unit to continue investing in the market and to continue developing innovative products to meet the requirements of several different types of customers.	standard
Marketing Execution	The success and "mind share" of the product in the WIPS market, including the installed base and market share, as well as the maturity and breadth of the organization's distribution channels. Also considered are the quality of customer case studies and references, and the level of interest from Gartner clients.	standard
Product/Service	Breadth of feature set is a key evaluation criterion. We specifically evaluated wireless intrusion detection and prevention capabilities, RF monitoring and reporting, and the level of integration of site-planning tools with ongoing security management tools.	high

Source: Gartner

Figure 1. MarketScope for Wireless LAN Intrusion Prevention Systems

	RATING				
	🟥	🟨	🟦	🟩	🟩
	Strong Negative	Caution	Promising	Positive	Strong Positive
AirDefense				x	
AirMagnet				x	
AirTight Networks				x	
Aruba Networks			x		
Cisco		x			

As of July 2008

Source: Gartner (July 2008)

Vendor Product/Service Analysis

AirDefense

Description: AirDefense introduced its first WIPS product in 2002, and it is the largest overlay WIPS vendor, remaining focused on this market. The WIPS product line consists of AirDefense Enterprise and AirDefense Personal for laptop protection. AirDefense also sells a laptop-based WLAN scanner to compete with AirMagnet's product, as well as WLAN-planning and survey tools.

Strengths: AirDefense has the highest level of visibility of all the overlay WIPS vendors and appears on most enterprise shortlists. AirDefense generally has been first to market with more-detailed security features and provides the most detailed information on wireless activity. AirDefense obtained Common Criteria certification for its product and has a strong presence in the government market. Its partnership with Motorola/Symbol gives it channel strength in nonoffice WLAN markets, such as transportation, manufacturing and utilities. Users give AirDefense high marks for support.

Challenges: Although AirDefense has greatly improved its default capabilities for alert classification, the broad array of features make it the most complex WIPS product offering on the market. Users often report that deploying and operating AirDefense requires more upfront effort than competing products. Although AirDefense's partnership with Motorola/Symbol gives it a strong entree into some vertical industries, Motorola is not a strong player against the two leading WLAN infrastructure vendors (Aruba and Cisco) in the broad WLAN infrastructure market, putting AirDefense at a disadvantage when WIPS is being considered as part of the infrastructure.

Optimal-use case: AirDefense is appropriate for security-focused buyers that are looking for overlay WIPS solutions that support detailed "lean forward" analysis of WLAN security and for infrastructure users of Motorola/Symbol WLAN gear.

Rating: Positive

AirMagnet

Description: With roots in the network sniffer market, AirMagnet was founded in 2001 and initially was focused on handheld and portable wireless network sniffers that frequently were used to detect unauthorized WLANs. The company moved into the WIPS market with AirMagnet Enterprise, adding distributed security monitoring and analysis to the established performance-monitoring and troubleshooting features. AirMagnet has a wide range of wireless analysis and monitoring products outside the WIPS space.

Strengths: As fits its beginnings, AirMagnet has the strongest range of WLAN performance-monitoring and troubleshooting capabilities in enterprise and mobile analyzer form. Users that selected AirMagnet generally report these factors as the primary reasons for selection. AirMagnet appears to have the closest working relationship and integration effort with Cisco, giving AirMagnet an edge where Cisco WLAN procurements are looking for overlay WIPS capabilities. AirMagnet has the second-highest level of competitive visibility in the Gartner client base, after AirDefense, and a significant number of clients purchase and rely on AirMagnet for IPS, taking advantage of its monitoring heritage.

Challenges: Although AirMagnet has the widest range of WLAN management tools, Gartner clients find that it does not have the breadth and depth of security features of its major overlay competitors. Users report that the security-reporting capabilities are less robust than those of the competition, driving the need to use external reporting systems, such as security information and event management products, for deeper security reporting. AirMagnet's major revenue streams come from the WLAN deployment and management tools side of the business, causing the engineering, marketing and channel strategies to be less focused on security.

Optimal-use case: AirMagnet is viable for all WIPS scenarios but is most appropriate for WLAN deployments where security and wireless network operations will be shared responsibilities and where one product will be used for both purposes.

Rating: Positive

AirTight Networks

Description: AirTight Networks is the youngest company in this MarketScope. It was established with a good vision for what people will buy, and this vision is earning it steady growth in financials and installed base. AirTight's competitive position is aggressive even though it has a short track record. AirTight's pure-play approach to sensor monitoring complements Cisco installations and comprehensively satisfies the expected functions of the market definition. Products include SpectraGuard Enterprise (WLAN IPS), SpectraGuard SAFE (endpoint agent) and SpectraGuard Planner for planning WLAN and WIPS deployments.

Strengths: Customer references report that the product is easy to set up and that it avoids false alarms by using multiple checks to classify rogues. The administrative-console help system can accommodate four different skill levels, from beginner to expert. The products are available in software as a service (SaaS) via SpectraGuard Online, as well as for direct purchase. AirTight has received Common Criteria certification in the U.S. AirTight's rapid setup is a powerful selling point when it makes the shortlist. OEM license relationships with WLAN infrastructure vendors such as Siemens, 3Com and Colubris contribute additional revenue in markets where these vendors have penetration.

Challenges: AirTight's relative youth in the market (four years) may cause concern for low-risk buyers (Type C companies). Being a pure-play sensor solution means that AirTight cannot pursue infrastructure sales against Cisco as Aruba and Meru do. Thus, AirTight is limited to selling its products as add-ons. However, this frees AirTight to concentrate solely on IPS matters and to sell into accounts held by dozens of incumbent WLAN vendors.

Optimal-use case: AirTight is appropriate for buyers that are looking for an easy-to-deploy solution and that are willing to take on a second wireless vendor to provide WIPS in exchange for strong security and rapid deployment with reduced overhead to set up and configure.

Rating: Positive

Aruba Networks

Description: Aruba Networks, established in 2002, focused on developing wireless mobility systems that addressed smart controllers and thinned-down APs. Early wins in WLANs drove Aruba to develop additional infrastructure-based security capabilities, and, in July 2007, Aruba acquired the RFprotect and BlueScanner WLAN security products from Network Chemistry, giving Aruba the ability to sell overlay wireless security monitoring as well. In 2008, Aruba acquired AirWave, which sold wireless system management tools that also had security monitoring capabilities. Aruba's WIPS product line consists of RFprotect Distributed (the overlay solution), RFprotect Mobile (a laptop-based Wi-Fi sniffer), RAPIDS (a rogue detection module that is part of the AirWave Wireless Management Suite) and the Aruba Wireless Intrusion Prevention module for use with the Mobility Controller's ArubaOS software (the infrastructure solution).

Strengths: Aruba's infrastructure-based WIPS capabilities are enhanced by the policy enhancement firewall that is part of the Aruba Mobility Controller. The Network Chemistry technology gives Aruba one of the easiest-to-use solutions for WIPS, and the AirWave acquisition provided additional security capabilities. Early on, Aruba had several government wins in wireless networking and has integration with the common access card, as well as current and pending Common Criteria certification. Aruba's references generally give its offerings high marks for ease of deployment and ease of management but chose Aruba mostly for WIPS because users were employing Aruba WLAN gear.

Challenges: Integrating Aruba, Network Chemistry and AirWave WIPS capabilities, all of which were developed independently, represents a large engineering effort. The disparate sources of its security technology causes Aruba's product approach to WIPS capabilities to be confusing. Because Aruba's success as a company is based primarily on selling its Mobility Controller and APs against other WLAN vendors (such as Cisco and Motorola), not on selling stand-alone WIPS products, Aruba must demonstrate that it will invest in moving the Network Chemistry-based overlay solution forward.

Optimal-use case: Aruba Networks' WIP module is appropriate for use with Aruba wireless networks, while the RFprotect Distributed product is an appropriate choice for the buyer whose primary driver is ease of use.

Rating: Promising

Cisco

Description: Cisco is a major player in the WLAN infrastructure market. Its infrastructure products include autonomous APs, lightweight APs managed by a controller and a platform for infrastructure management. Cisco's security product provides core IPS functions.

Strengths: Cisco's production solutions are common shortlist contenders in enterprises of all sizes and are the most widely deployed in the enterprise WLAN infrastructure market, generally capturing two-thirds of the market. Cisco's APs detect and recognize the widest range of IT and consumer wireless protocols and signals of any vendor on the market. Cisco has invested heavily in improving its WLAN security capabilities and has aggressively pursued the integration of security and management for wireless and wired networking as part of its unified network strategy.

Challenges: Cisco's WIPS is not communicated effectively in competitive sales situations. Despite Cisco's IPS and management acquisitions, as well as internal developments to improve wireless security, Gartner clients find Cisco's unified network strategy to be complex and typically do not recognize or understand how to take advantage of the WIPS capabilities. For example, in a unified network scenario, the user must deal with cross-configurations of standard and lightweight APs used in production and hybrid modes, Wireless LAN Controllers (WLCs), Wireless Control System (WCS) console, Wireless LAN Controllers (WLCs), Mobility Service Engines (MSEs), Cisco MARS and others. Clients often perceive the incremental cost of adding a third-party product to be the easiest way to supplement Wi-Fi management and security for a Cisco network. This belief is complicated by Cisco's tendency to endorse partners in its WLAN management and security sales, most recently AirMagnet. Clients also report other persistent perception problems, including a lack of awareness as to the extent to which Cisco has advanced its internal integration of wired/WIPS capability. Cisco recommends that buyers use production APs for listening purposes, but it has been unable to interrupt growth from pure-play WLAN IPS companies that continue to make compelling arguments for dedicated sensors. In our opinion, Cisco must overhaul its wireless security client education and sales messages.

Optimal-use case: Cisco is a strong choice for production wireless-access infrastructure-based monitoring when deploying dedicated sensors isn't feasible. Cisco can be used for high-security, managed environments, although client perceptions continue to favor Cisco for low-security and simple management environments. Extensive case study interviews indicate that buyers seeking strong wireless security in 2008 will continue to consider third-party products.

Rating: Caution

RECOMMENDED READING

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

"What to Look for in a Wireless Intrusion Prevention System"

"Magic Quadrant for Wireless LAN Infrastructure, 2007"

"Introduction to Wi-Fi Security Best Practices"

"Wi-Fi Security Best Practices for Traveling Employees"

"Wi-Fi Security Best Practices for Company Offices"

"Wi-Fi Security Best Practices for Employees Working at Home"

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Gartner MarketScope Defined

Gartner's MarketScope provides specific guidance for users who are deploying, or have deployed, products or services. A Gartner MarketScope rating does not imply that the vendor meets all, few or none of the evaluation criteria. The Gartner MarketScope evaluation is based on a weighted evaluation of a vendor's products in comparison with the evaluation criteria. Consider

Gartner's criteria as they apply to your specific requirements. Contact Gartner to discuss how this evaluation may affect your specific needs.

In the below table, the various ratings are defined:

MarketScope Rating Framework

Strong Positive
Is viewed as a provider of strategic products, services or solutions:

- *Customers:* Continue with planned investments.
- *Potential customers:* Consider this vendor a strong choice for strategic investments.

Positive
Demonstrates strength in specific areas, but execution in one or more areas may still be developing or inconsistent with other areas of performance:

- *Customers:* Continue planned investments.
- *Potential customers*: Consider this vendor a viable choice for strategic or tactical investments, while planning for known limitations.

Promising
Shows potential in specific areas; however, execution is inconsistent:

- *Customers:* Consider the short- and long-term impact of possible changes in status.
- *Potential customers:* Plan for and be aware of issues and opportunities related to the evolution and maturity of this vendor.

Caution
Faces challenges in one or more areas.

- *Customers:* Understand challenges in relevant areas, and develop contingency plans based on risk tolerance and possible business impact.
- *Potential customers:* Account for the vendor's challenges as part of due diligence.

Strong Negative
Has difficulty responding to problems in multiple areas.

- *Customers:* Execute risk mitigation plans and contingency options.
- *Potential customers:* Consider this vendor only for tactical investment with short-term, rapid payback.

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509